Bolt Beranek and Newman Inc.

(12)

Report No. 5580

AD-A145 348

Combined Quarterly Technical Report No. 32

Pluribus Satellite IMP Development
Mobile Access Terminal Network

February 1984

Prepared for:
Defense Advanced Research Projects Agency

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER	2. GOVT ACCESSION NO. A145 348	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) Combined Quarterly Technical Report No. 32		5. TYPE OF REPORT & PERIOD COVERED Quarterly Technical 11/1/83 - 1/31/84
		6. PERFORMING ORG. REPORT NUMBER 5580
7. AUTHOR(s)		8. CONTRACT OR GRANT NUMBER(s) MDA903-80-C-0353 N00039-81-C-0408
9. PERFORMING ORGANIZATION NAME AND ADDRESS Bolt Beranek and Newman Inc. 10 Moulton Street Cambridge, MA 06238		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS Arpa Order No. 3214
11. CONTROLLING OFFICE NAME AND ADDRESS Defense Advanced Research Projects Agency 1400 Wilson Boulevard Arlington, VA 22209		12. REPORT DATE February 1984 13. NUMBER OF PAGES 34
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office) DSSW Room ID The Pentagon Washington, DC 20310 NAVALEX Washington, DC 20360		15. SECURITY CLASS. (of this report) UNCLASSIFIED 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE
16. DISTRIBUTION STATEMENT (of this Report) APPROVED FOR PUBLIC RELEASE/DISTRIBUTION UNLIMITED		
17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)		
18. SUPPLEMENTARY NOTES		
19. KEY WORDS (Continue on reverse side if necessary and identify by block number) Computer networks, packets, packet broadcast, satellite communication, gateways, Pluribus Satellite IMP, shipboard communications, ARPANET, Internet.		
20. ABSTRACT (Continue on reverse side if necessary and identify by block number) This Quarterly Technical Reprot describes work on the development of Pluribus Satellite IMPs: and on shipboard satellite communications.		

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED

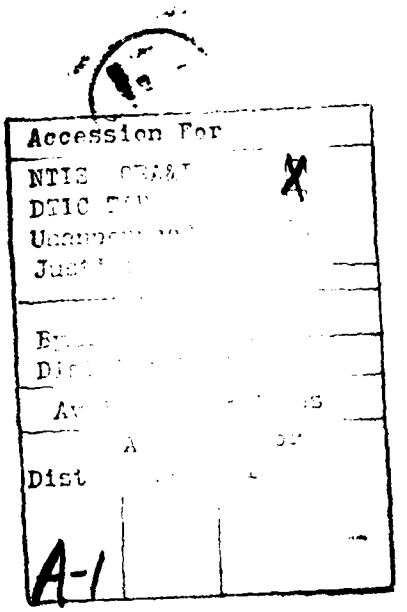
SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

Report No. 5580

COMBINED QUARTERLY TECHNICAL REPORT NO. 32

PLURIBUS SATELLITE IMP DEVELOPMENT
MOBILE ACCESS TERMINAL NETWORK

February 1984



This research was supported by the Defense Advanced Research Projects Agency under the following contracts:

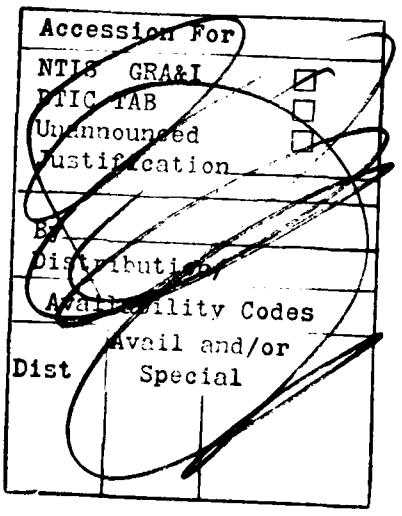
MDA903-80-C-0353, ARPA Order No. 3214
N00039-84-C-0408

Submitted to:

Director
Defense Advanced Research Projects Agency
1400 Wilson Boulevard
Arlington, VA 22209

Attention: Program Management

Table of Contents



FIGURES

1 INTRODUCTION

This Quarterly Technical Report is the current edition in a series of reports which describe the work being performed at BBN in fulfillment of several ARPA work statements. This QTR covers work on several ARPA-sponsored projects including (1) development of the Pluribus Satellite IMP; and (2) development of the Mobile Access Terminal Network. This work is described in this single Quarterly Technical Report with the permission of the Defense Advance Research Projects Agency. Some of this work is a continuation of efforts previously reported on under contracts DAHC15-69-C-0179, F08606-73-C-0027, F08606-75-C-0032, MDA903-76-C-0214, MDA903-76-C-0252, N00039-79-C-0386, and N00039-78-C-0405, and N00039-81-C-0408.

2 PLURIBUS SATELLITE IMP DEVELOPMENT

This Quarterly Technical Report discusses recent progress in the development and systems integration of the Wideband Network. It covers systems integration work done at several Wideband Network task force meetings, improvements made to the PSAT software, and progress made in the development of the BSAT. This QTR includes a detailed discussion of the design of the PSAT translator program which will be used to connect the BSAT, running in Voice Funnel hardware, up to an ESI and earth terminal for test and debugging purposes.

2.1 Wideband Network Systems Integration Activities

The Wideband Network task force convened for network debugging sessions several times during the quarter. During the week of November 14, they met at Lincoln Laboratory to work on problems associated with three site network operations. Multisite operation uncovered an ESI problem which disrupted the network when several consecutive long outoing messages were transmitted by the PSAT to the ESI. The problem was corrected by increasing the ESI's internal uplink delay from 3 to 6 milliseconds.

Linkabit finished debugging the ESI-A at ISI during the month of November. By the end of the month the ESI-A had been operating stably on the network for many days. In the course of working with Linkabit to debug the ESI-A, a near-end crosstalk problem was discovered with the PSAT Satellite Modem Interface (SMI). This problem was corrected by replacing the internal SMI-to-PSAT Fantail flat ribbon cable by a cable made up of twisted pairs.

During December, an additional site was added to the network. BBN, Lincoln Laboratory, and Linkabit visited Ft. Monmouth on December 5-7, installed an ESI, and successfully brought the site up on the air. A PSAT software bug was identified which disrupted normal network operation when the Ft. Monmouth site was not the leader on the satellite channel.

Significant progress was made in Wideband Network systems integration during January. On January 9, BBN found and corrected the PSAT software bug which prevented Ft. Monmouth from operating on the channel unless it was leader. A site-dependent pointer was accessing a table incorrectly. Correcting this bug allowed Lincoln to conduct extensive speech testing between Ft. Monmouth and Lincoln using their Packet-to-Circuit Interfaces (PCI) at both sites.

2.2 Wideband Network Operations and Maintenance

Several PSAT hardware problems were encountered during the quarter. The hardware problems encountered with the ISI PSAT during November, a failed power supply, a non-functioning processor, and a faulty backplane, were repaired on December 4. Additional hardware problems were encountered with the ISI PSAT on December 18. The problems were finally traced to a set of faulty bus couplers which were replaced on December 28. A host port in the RADC PSAT, which had failed at the end of November, was replaced on December 1. On December 5 the RADC earth terminal high power amplifier (HPA) went into standby mode. This condition was not cleared by Western Union until December 12.

The SRI PSAT experienced hardware problems during December. Although significant effort was expended during the month trying to track down the cause of the problems, progress was slow, and the problems remained unresolved at the end of the month. The hardware problems were finally traced to a set of bad bus couplers and memory boards in early January and the PSAT was returned to operational status on January 8. An ESI was installed at SRI on January 13; however, a problem was discovered with the High Speed Packet Modem (HSPM). Representatives from BBN, Lincoln, ISI, and Linkabit visited SRI on January 19-20 and replaced the HSPM with the Burst Test Modem (BTM). When the site was brought up on the channel, problems were encountered with the

earth terminal's high power amplifier (HPA). It was found to be operating at a very low output power level. The channel bit error rate (BER) was measured at 1x10**-3. During the visit, ISI repaired the Switched Telephone Network Interface (STNI) which they had installed in a Packet Voice Terminal (PVT) at SRI, and, with rate 1/2 coding, it was possible to make a telephone call of acceptable quality over the channel in spite of the high bit error rate. At the end of the quarter, Linkabit was still working on repairing the modem, and Western Union was working on the earth terminal.

2.3 BSAT Software Development

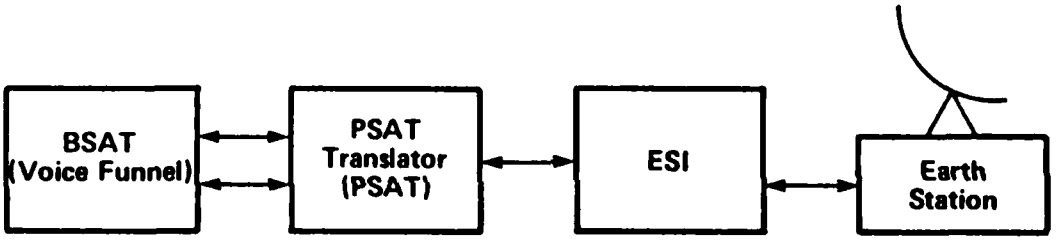
BSAT software development during the quarter focused on the coding and debugging of the software-based satellite channel simulator (described in a previous QTR), on the debugging of the datagram scheduling code, on the coding of routines to handle stream setups and to manipulate the stream databases, and on the design of the PSAT Translator program. An overview of the PSAT translator is given in the next section.

2.4 Design of the PSAT Translator Program

Currently the PSAT is connected to the ESI and earth terminal equipment via a Satellite Modem Interface (SMI). The SMI provides a satellite channel clock to precisely time the transmission and reception of channel bursts. It also contains logic to generate and check 32 bit CRCs for error detection. The PSAT SMI exchanges data with the ESI using a count-based variant of the Arpanet VDH-style protocol. For the BSAT, BBN has proposed to develop a new HDLC based interface, the Butterfly Satellite Modem Interface (BSMI) to communicate with a new ESI-B currently being developed by Linkabit. The precise timing functions will be moved to the ESI-B. However, the CRC error checking will still be performed by BSAT.

To allow testing of the BSAT software before either the ESI-B or BSMI are available, BBN has proposed to develop a Pluribus program for the PSAT known as the PSAT Translator. The PSAT Translator will allow the BSAT running in Voice Funnel hardware, currently at several Wideband Network sites, to be connected to the current ESIs and ESI-As, using the PSAT's SMI. Figure 1 shows the configuration in which the PSAT translator will be used.

In the PSAT, transmission of scheduled bursts is performed by the Satellite Modem Interface (SMI). The SMI transmits a



Configuration for testing the BSAT using the PSAT
Figure 1

burst to the ESI-A upon timeout of a time-to-go stamp on the pending burst. The time reference for the SMI is based on a clock signal provided by the ESI-A. When the ESI-B is developed, it will perform this timeout function. The PSAT Translator accepts scheduled bursts from the BSAT and performs the format and time conversions necessary for proper time out and transmission to the ESI-A. For traffic received from the satellite channel, the PSAT Translator also performs the proper format and time conversions for transmission to the BSAT. The PSAT Translator combines with the current ESI or ESI-A to simulate the function which the ESI-B will have.

2.4.1 PSAT Translthe PSAT Translator is taken largely from the Host Protocol Module (HPM) of the PSAT. In the PSAT HPM, input and output are accomplished by the MsgIn and MsgOut device drivers. MsgIn and MsgOut perform I/O driver functions associated with message-to-buffer conversion and device control. In the PSAT, the MsgIn and MsgOut drivers control I/O only between the PSAT and hosts. However, in the PSAT Translator, this I/O mechanism has been extended to control both the host interface and the satellite interface. Thus two MsgIn/MsgOut driver pairs exist, one attached to the High Speed Modem (HSM) used for communication with the BSAT and another pair

attached to the Satellite Modem Interface (SMI) used for communication with the ESI-A.

As in the PSAT HPM, MsgIn and MsgOut provide message I/O service to message level input and output processes, HstIn and HstOut. In the PSAT, HstIn and HstOut perform Host Access Protocol (HAP) message processing. In the PSAT Translator, HstIn and HstOut have been altered to perform the burst processing required to convert ESI-B-type bursts into ESI-A-type bursts. Since there are two pairs of device drivers, there are also two HstIn/HstOut pair analogues called XlatIn and XlatOut. To distinguish between pairs, the XlatIn/XlatOut processes associated with the High Speed Modem are referred to as BSAT XlatIn and BSAT XlatOut. The processes associated with the Satellite Modem Interface are referred to as Satellite XlatIn and Satellite XlatOut. Communication between the BSAT XlatIn process and the Satellite XlatOut process is accomplished through a message queue. This queue is called UpQ, since it provides uplink communication between message level I/O processes. Similarly, communication between the Satellite XlatIn process and the BSAT XlatOut process is accomplished through a queue called DnQ, so named for its downlink role. (See Figures 2 and 3)

In the PSAT Translator, the conversion of ESI-B-type bursts into ESI-A-type bursts is performed in the Satellite and BSAT XlatIn processes. The XlatOut processes function only as message passers.

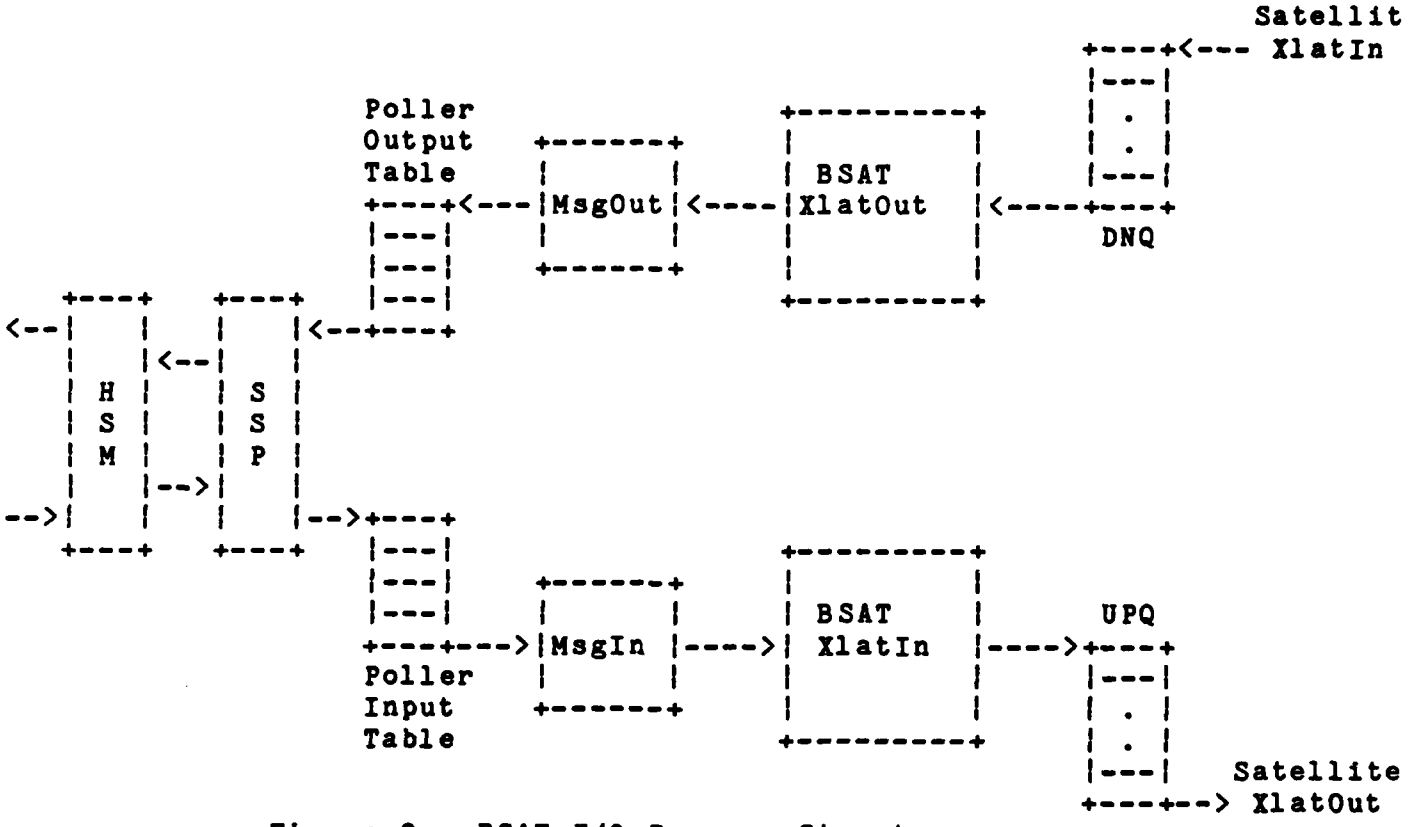


Figure 2 . BSAT I/O Process Structure

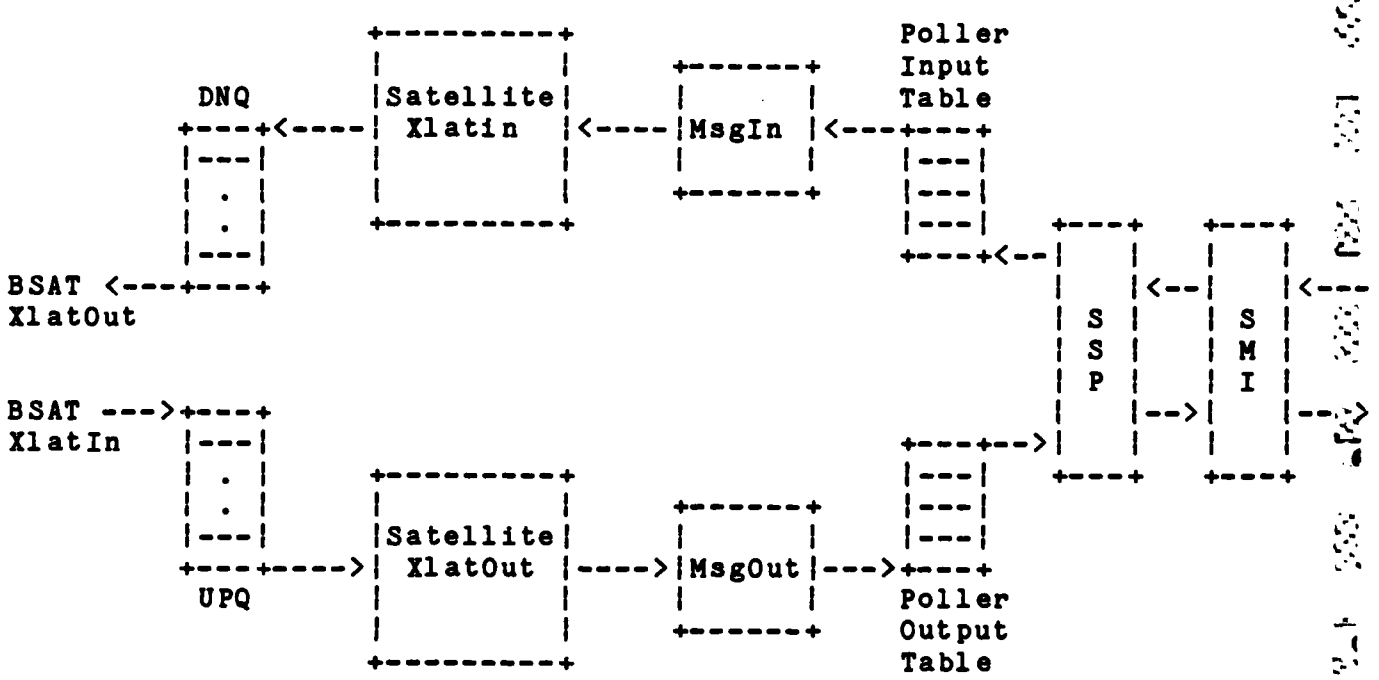
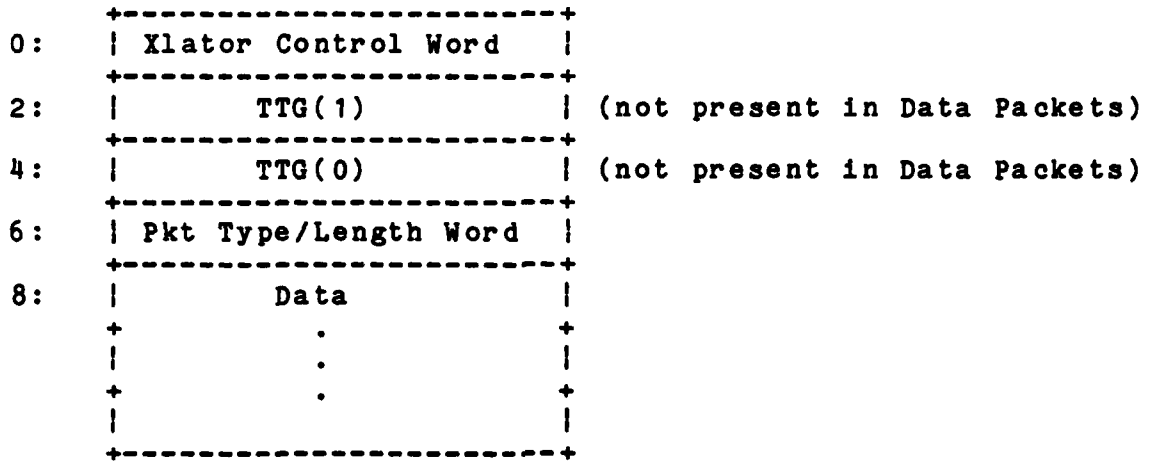


Figure 3 . Satellite I/O Process Structure

2.4.2 PSAT Translator Protocol

All packets passing between the BSAT and the PSAT Translator are of the following format:



The PSAT Translator control word communicates various status and label information between the BSAT and PSAT Translator. The fields are defined as follows:

Bit 0 (lsb):	Last Packet of Burst
Bit 1:	Local Time Update Request
Bit 2:	Data Packet
Bit 3-9:	(Not currently used)
Bit 10:	Hard ESI Reset Request
Bit 11-13:	(Not currently used)
Bit 14-15:	PSAT Translator Loop Status

The 'Last Packet of Burst' field indicates that the current packet is the final packet in the current burst. For the ESI-A, a burst may consist of one or more packets: a control packet followed by one or more data packets. The PSAT Translator uses this bit to signal completion of burst assembly to the Super Sue Poller. When signalled, the Super Sue Poller will initiate DMA transfer of all packets in the round-robin table through the Satellite Modem Interface to the ESI-A. The 'Local Time Update Request' field indicates that the PSAT Translator should return a local control packet of type ESI-to-BSAT to the BSAT containing the current local time as maintained by the SMI. To maintain accurate channel timing, the BSAT requires periodic updates of local time.

The 'Data Packet' field indicates that the current packet is a data packet as distinguished from an ESI-A control packet.

The 'Hard ESI-A Reset Request' field indicates to the PSAT that it should perform a hard reset of the ESI-A. A hard reset consists of toggling a control wire in the SMI/ESI-A cable.

The 'PSAT Translator Loop State' indicates the current Translator loop status. Bit 14 indicates SMI loop and Bit 15 indicates TR loop. Both bits clear indicates no loop. Both bits set indicates PSAT Translator Software loop.

3 TACTICAL PACKET SATELLITE NETWORK

The Mobile Access Terminal Network (MATNET) will hereafter be designated as the Tactical Packet Satellite Network (TACNET). After renewal of the contract for our participation in further TACNET development, we conducted a study of suitable architectures for the second-generation TACNET system. In this Quarterly Technical Report, we provide preliminary results of our architectural investigations, with emphasis on TACNET security issues.

The new TACNET Satellite IMP (SIMP) will be implemented on modular BBN Butterfly Multiprocessor hardware. The multiprocessor modularity will provide the flexibility to handle a variety of diverse system requirements, as well as the expandability required to provide increased throughput under heavier system traffic loads. The multiprocessor design will allow a variety of hosts to be connected into the network and will allow for several types of radio channel equipment to be serviced simultaneously. Given that TACNET will be required to carry classified data in an operational Navy environment, our design will provide the capability to include end-to-end network security devices, as well as separate satellite channel encryption devices.

3.1 The Butterfly Multiprocessor

The Butterfly Multiprocessor was originally developed for the Voice Funnel application in the DARPA Wideband Satellite Network. In that capacity it acts as a high performance Internet Gateway for the routing of speech traffic using the ST Internet packet speech protocol. It also aggregates small speech and video packets into larger packets for transmission on the satellite channel by the Pluribus Satellite IMP (PSAT). At this time six 10-processor Voice Funnels have been built for the Wideband Network. A Butterfly-based version of the Internet Gateway is under development for the DARPA Internet project. Initial deployment of these gateways will begin in early 1985. A new Satellite IMP, the BSAT, based on the Butterfly Multiprocessor, is currently under development for the Wideband Network. The software to be developed for the new TACNET Satellite IMP will draw heavily on our experience in developing the BSAT.

The Butterfly Multiprocessor consists of processor nodes interconnected by a switch whose paths are patterned after the Fast Fourier Transform "Butterfly" network. Each processor node includes a Motorola MC68000 microprocessor with a bit-sliced microprogrammed coprocessor, up to 4 Mbytes of local memory, a memory management unit, optional high-speed intelligent chained-DMA I/O channels, and an interface to the Butterfly switch. The

system is expandable by adding more processor and switch nodes (described below).

The current Butterfly switch is built up from radix-4 switch nodes. It contains 4-bit-wide data paths and runs at a clock rate of 8 Mhz to achieve a 32 Mb/s throughput. All memory in the system is global in the sense that it is directly accessible by each of the processor nodes via the switch.

Each I/O device in the system is associated with a single processor node. Several specialized communications-oriented I/O devices either have been designed or are in the process of being designed for the Butterfly. These include a synchronous (four channels) and asynchronous (four channels) serial I/O board, an interface to the satellite channel equipment for the Wideband Network, and an interface to a T1 circuit-switched telephone network. In addition, we have developed a Multibus adaptor which will allow a wide variety of standard Multibus compatible I/O devices to be connected to a Butterfly processor node.

An operating system, Chrysalis, has been developed for the Butterfly to handle real-time communications tasks in the multiprocessor environment. Chrysalis supports the execution of independent user-level processes written in the C programming language. Chrysalis provides virtual and physical address space management and protection, per-processor-node process scheduling,

interprocess communication, synchronization, and task distribution mechanisms ("events" and "dual queues"), and system timers. Chrysalis itself is written in C with many of its underlying mechanisms implemented on the microcoded coprocessor for significant performance enhancement.

Detailed documentation of the Butterfly Multiprocessor and the Chrysalis operating system can be found in the series of BBN Quarterly Technical Reports provided to DARPA for The Voice Funnel project.

3.2 Overview of TACNET Security Issues

It has been recognized for some time that the imposition of network security devices into the current C/30-based system has severely handicapped the system integration. In addition, the nature of the security devices has interfered with the use of the TACNET system in many of the Navy's demonstration and testbed environments. We realize that for any packet-switched satellite communication system to gain acceptance and be used in a Naval operational environment, the issue of network security must be addressed and solved. It must be included and dealt with throughout the system design and development phases and not just tacked on shortly before declaring the system operational. It is for this reason that our preliminary investigations have resulted

in an evolutionary system that will first integrate packet satellite technology into the Navy's shipboard and shore-based environments with appropriate security measures for the testbed environment, and will later replace these initial security devices with more sophisticated security devices as the requirements of the operational mission are defined.

The initial version of the new TACNET system will be used in the testbed environment. It will not carry any sensitive data and will not include any security devices. This system will be used for the development of interfaces for the various radios that are contemplated for use by TACNET, for the development of appropriate codecs and interleavers for noise immunity, and for continued work on the PODA algorithms.

The TACNET Satellite IMP will include support for HDLC physical host interfaces. Such interfaces are compatible with the currently planned family of packet-switched network end-to-end security devices. In the testbed demonstration environment, it may be necessary to protect unclassified sensitive data. We would use a DES-based security device in the host-to-SIMP link to provide protection of such data, and explore the impact of end-to-end security devices on the operation of the network.

As the classification of the data carried by TACNET increased to the SECRET level, we would exchange the DES-based

devices for Internet Private Line Interfaces (IPLIs). The IPLIs will support the same host protocol as the DES devices and will be interchangeable. The introduction of SECRET data into the network and the IPLI in particular will require an increase in the network's physical security (red-black engineered environment, TEMPEST, etc.).

In anticipation of having TACNET carry still higher level classified data in an operational system, we propose to design the system with the capability of introducing some form of encryption on the satellite channel at a future time. In particular, we propose a separation of the satellite channel protocol functions from the satellite link transmission/reception functions, the different sets of functions being performed in separate Butterfly processor nodes. When encryption is required on the satellite channel, we will interpose a DES-based security device between the two subsystems. This will allow us to cover the addressing portions of the messages on the satellite channel in order to guard against traffic analysis. The Butterfly processor(s) on the satellite channel side of the security device will only be executing software controlling the codec/interleaver and the radio(s). The processor node(s) on the other side of the security device will run the satellite channel protocol module (i.e., will perform the scheduling of the satellite channel).

The architecture of the DES-based security device as described below will allow for a much more sophisticated cryptographic bypass than is provided in the current C/30-based system. In a real operational system handling data that is classified as TOP SECRET and above, we anticipate replacing the DES-based device in the satellite channel path with one of the encryption devices from the Blacker program (with software modifications for the TACNET application).

3.3 Detailed Examination of Two of the Proposed Systems

In this section, we will discuss two important stages in our evolutionary plan: one in which only end-to-end encryption on the host links is used, and one in which some type of encryption (with an appropriate bypass) is used to protect addressing information on the satellite channel itself in order to guard against traffic analysis.

In both of the architectures to be described, the need to protect the DATA content of classified traffic or sensitive unclassified traffic can be satisfied by the use of encryption devices external to the TACNET system. IPLIs can be used in the classified case, and DES-based devices can be used in the latter privacy-only case. Both of these devices can be used for end-to-end encryption across many interconnected networks, so that

they will not necessarily be directly connected to TACNET host ports. If an IPLI or DES-based device is connected to a TACNET host port, the encryption device will interface to the network in the same fashion as any other external host. Since the provision of message DATA content protection is a standard use for which the security devices are being developed, there may be little or no NSA involvement required when they are so used by the TACNET application.

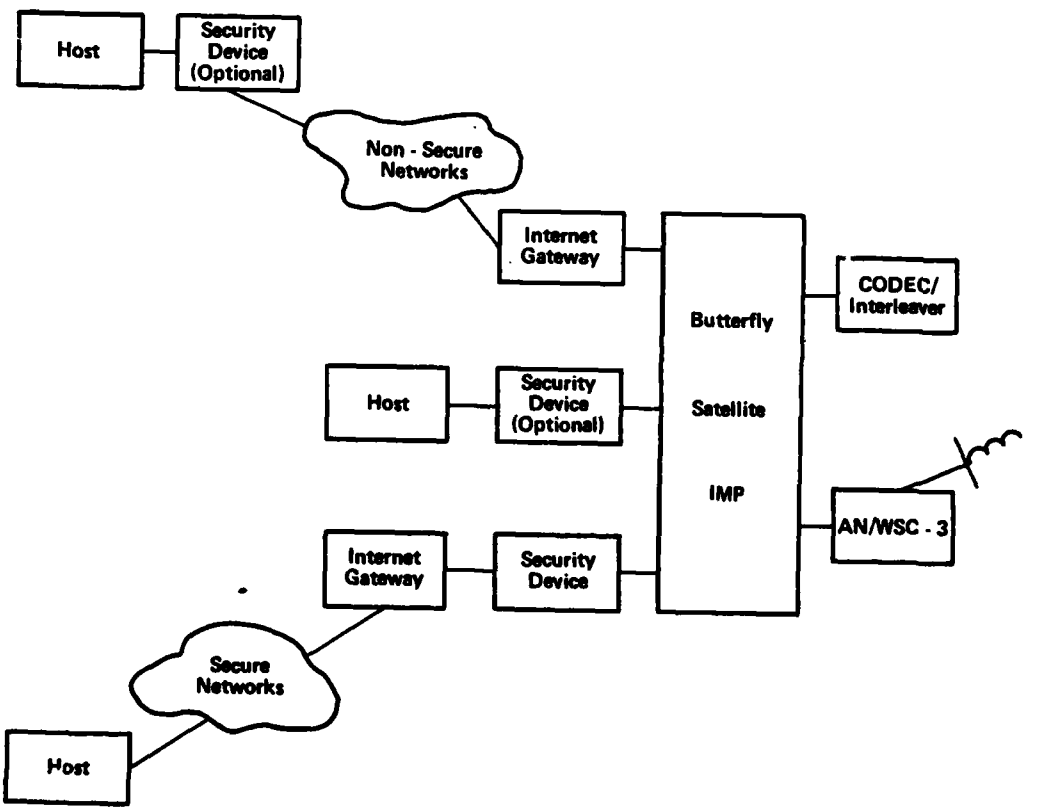
3.3.1 System A

This new TACNET architecture does not address the traffic analysis protection requirement: It is assumed in this case that the system will never be expected to handle (cipher-text OR plain-text) messages whose addressing information must be concealed. The most significant aspect of System A is that it contains no internal encryption devices, permitting a system architecture which is much simpler than that used in the current C/30-based system and requiring no NSA approval of any of the TACNET components. In such an "all black" system, the processing components performing the satellite channel scheduling have easy access to all of the known information on the state of the channel, since their communications with the codec/interleaver and AN/WSC-3 radio interfaces are unencumbered by encryption

devices or limited-bandwidth bypasses. This permits complete channel-state reporting to the network monitoring site, and may also simplify the implementation of any solutions to the contention packet discrimination problem. Additionally, no communications bandwidth is lost within the TACNET system because of encryption overhead (per-packet initialization vectors, fill, etc.) to possible encryption device alarms.

A block diagram of System A is shown in Figure 4. The complete host message routing, satellite channel protocol, and Satellite IMP monitor/control functions, as well as the higher level parts of the host interfacing, codec/interleaver control, and AN/WSC-3 control functions will be implemented as C-language software which will be compiled for execution on the MC68000 processors resident on the Butterfly processor nodes.

HDLC link-level host interfaces will be provided. Although the current Butterfly I/O board provides HDLC ports, it may be most flexible (given the various system I/O requirements) to use Multibus-compatible I/O boards. These host interface boards each contain an HDLC and an 1822 port driven by a microcodable processor. The on-board processor could be microcoded to interact with the Chrysalis operating system so as to eliminate the low-level host-I/O processing burden that would otherwise be



Block Diagram of System A
Figure 4

placed on the MC68000 application software.

The use of Multibus-compatible boards by a Butterfly processor node requires a Multibus adaptor board to perform the conversion between the standard Butterfly I/O bus (the BIOLINK) and the Multibus. Such a board has been developed for Butterfly-based Internet Gateway.

The encoding/decoding and interleaving/deinterleaving functions will be provided by another Multibus-compatible device. BBN will evaluate commercially available codecs and interleavers to determine if they are suitable and available with the appropriate level of vendor support for the TACNET system. If no suitable commercially available codecs and interleavers are found, BBN will undertake to develop an appropriate codec and interleaver.

The AN/WSC-3 interface would also be located on the Multibus. Its functions would include transmitter keying, modem preamble generation, unique word correlation, maintenance of the local transmit/receive clock, etc. A key criterion for the selection or design of the codec/interleaver and AN/WSC-3 interfaces will be their ability to provide intelligent DMA-based interfaces to Butterfly processor nodes to reduce the processing burden on the MC68000 device driver software.

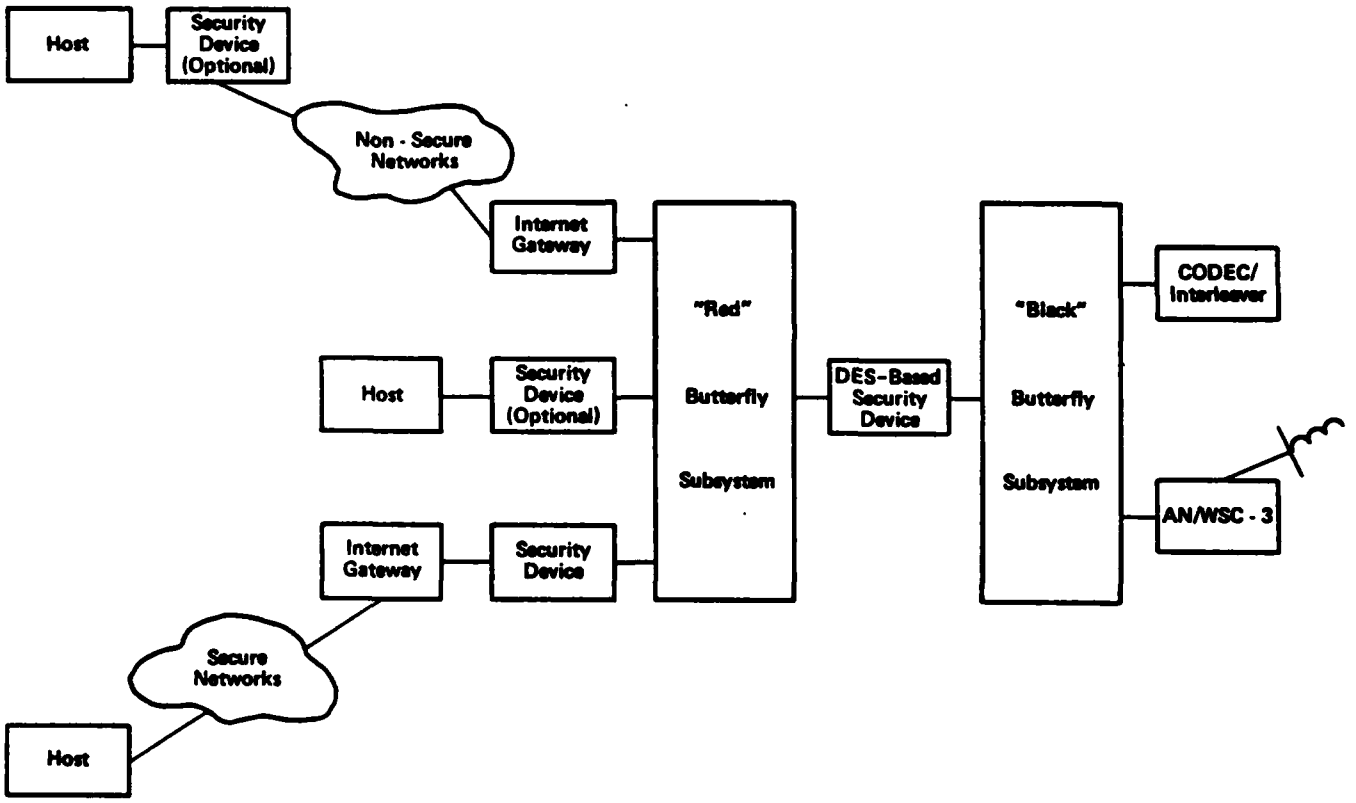
3.3.2 System B

Changes must be made to the System A architecture if TACNET will be required to handle messages whose addressing information must be encrypted before being broadcast over the satellite channel. The resulting architecture (such as "System B", described below) requires some form of encryption device(s) to be placed within each TACNET Satellite IMP. The exact form of encryption device used depends on, among other factors, whether the addressing information is categorized as classified or unclassified (but sensitive). In the former case, a high-grade COMSEC device would be used for address encryption; in the latter case a privacy-only device using DES may suffice. Some form of NSA approval would be required in either of these cases, although the standards used for the approval would be different for the two general device types. The placement of any encryption devices within TACNET adds some complexity to the system and may affect system throughput in much the same way as it does in the current C/30-based system, i.e., the system divides into a "red" and a "black" subsystem, the processors in the two subsystems communicating through the encryption device (whose operational mode may add to the system overhead) and a limited-bandwidth bypass.

It must be stressed that the degree of difficulty inherent in providing address information encryption within TACNET (due to

obtaining/developing NSA approved devices and due to encryption device bypass constraints) is strongly affected by the type of device used, and hence by the classification of the addressing information. (In those cases where a DES-based device is allowable the difficulty is minimized, resulting in a system that is simpler and more flexible than the current C/30 system. Such a DES-based architecture is represented by System B, which is described below.) If the new TACNET system will be considered to have an operational role in Naval communications, and in this role will process messages whose addressing information must be treated as classified independent of the message data content, then the relatively complex route of using a high-grade COMSEC device must be taken. On the other hand, if the new TACNET system's role is solely one of demonstration of concept, and as such the address information is unclassified, then the simpler DES-oriented privacy-only route or the even simpler "all black" system route (System A) would suffice.

A block diagram of System B is shown in Figure 5. System B's "red" side contains the same Butterfly processor nodes and host interfaces as System A. The "black" side of System B consists of Butterfly processors which are connected to the codec/interleaver and AN/WSC-3 interface devices. The red subsystem performs all required functions other than



Block Diagram of System B
Figure 5

codec/interleaver and AN/WSC-3 control; the latter are handled by the black subsystem.

The red and black processor nodes communicate using DES-based security hardware which will be connected to the nodes via HDLC interfaces. The security hardware will be contained in a separate box and will be identical to that being developed for other applications by BBN. Modifications will be made to the C-language software which executes on the MC68000 that is contained within the security device. Such modifications are required because of differences between the TACNET application and other applications using the DES-based device (which generally have the security device located between a host and its packet-switch node). The security device's software would be set up to pass control and status messages between the red and black processor nodes without performing any encryption or decryption operations on such messages, thereby providing a high-bandwidth bypass. The software will also bypass certain control data prepended to packets to be broadcast over or received from the satellite channel, e.g., packet transmission/reception timestamps. Such bypass capability provides a far simpler and much more flexible red/black subsystem interface than that contained in the C/30-based system.

Separately packaged DES hardware is used in System B to expedite the required NSA approval for its use in the TACNET

application as a privacy device under Federal Standard 1027. Since 1027 approval is anticipated for some of the other DES device applications, and since the TACNET software modifications are expected to be minimal, approval should not be difficult. The alternative route of using a DES board as a peripheral device directly accessible by a Butterfly processor node is not being taken, since it would probably require 1027 approval for the entire Butterfly system.

DISTRIBUTION

ARPA
Director (3 copies)
Defense Advanced Research Projects Agency
1400 Wilson Blvd.
Arlington, VA 22209
Attn: Program Manager
R. Kahn
R. Ohlander
B. Leiner

DEFENSE DOCUMENTATION CENTER (12 copies)
Cameron Station
Alexandria, VA 22314

DEFENSE COMMUNICATIONS ENGINEERING CENTER
1860 Wiehle Road
Reston, VA 22090
Attn: Maj. J. Fredricks

DEPARTMENT OF DEFENSE
9800 Savage Road
Ft. Meade, MD 20755
Attn: R. McFarland C132 (2 copies)

DEFENSE COMMUNICATIONS AGENCY
8th and South Courthouse Road
Arlington, VA 22204
Attn: Code B645
Glynn Parker, Code B626

NAVAL ELECTRONIC SYSTEMS COMMAND
Department of the Navy
Washington, DC 20360
Attn: B. Hughes, Code 6111
F. Deckelman, Code 6131

MIT Laboratory for Computer Science
545 Technology Square
Cambridge, MA 02138
Attn: D. Clark

MIT Lincoln Laboratory
244 Woods Street
Lexington, MA 02173
Attn: C. Weinstein

DISTRIBUTION cont'd

USC Information Sciences Institute
4676 Admiralty Way
Marina Del Rey, CA 90291
Attn: D. Cohen
S. Casner

DISTRIBUTION cont'd

BOLT BERANEK AND NEWMAN INC.
1300 North 17th Street
Arlington, VA 22209
Attn: E. Wolf

BOLT BERANEK AND NEWMAN INC.
10 Moulton Street
Cambridge, MA 02238

S. Blumenthal
M. Brescia
R. Bressler
J. Byrd
P. Cudhea
A. Echenique
R. Edmiston
W. Edmond
L. Evenchik
G. Falk
J. Goodhue
S. Groff
R. Gurwitz
J. Haverty
F. Heart
J. Herman
R. Hinden
D. Hunt
S. Kent
A. McKenzie
D. Melone
W. Milliken
R. Newman
M. Nodine
R. Rettberg
H. Rising
J. Robinson
E. Rosen
P. Santos
J. Sax
S. Storch
R. Thomas
R. Waters
B. Woznick
Library